American
Megatrends

Public Document (PUB)

An Introduction to UEFI

An overview of Unified EFI (UEFI) and how it applies to BIOS products

Updated 2011-02-10

LEGAL

Disclaimer
- This publication contains proprietary information which is protected by copyright. No part of this publication may be reproduced, transcribed, stored in a retrieval system, translated into any language or computer language, or transmitted in any form whatsoever without the prior written consent of the publisher, American Megatrends, Inc. American Megatrends, Inc. retains the right to update, change, modify this publication at any time, without notice.

For Additional Information
- Call American Megatrends, Inc. at 1-800-828-9264 for additional information.

Limitations of Liability
- In no event shall American Megatrends be held liable for any loss, expenses, or damages of any kind whatsoever, whether direct, indirect, incidental, or consequential, arising from the design or use of this product or the support materials provided with the product.

Limited Warranty
- No warranties are made, either express or implied, with regard to the contents of this work, its merchantability, or fitness for a particular use. American Megatrends assumes no responsibility for errors and omissions or for the uses made of the material contained herein or reader decisions based on such use.

Trademark and Copyright Acknowledgments
- Copyright ©2011 American Megatrends, Inc. All Rights Reserved.
- American Megatrends, Inc., 5555 Oakbrook Parkway, Suite 200, Norcross, GA 30093
- All product names used in this publication are for identification purposes only and are trademarks of their respective Companies.

BIOS - KEY TO A SOLID PLATFORM

BIOS offers the compatibility between the hardware & operating system that makes the x86 platform today's most flexible computing architecture.

Pre-boot Value Add

Maximum OS-to-BIOS Compatibility

Platform Initialization

UEFI brings modern software methods and C-based programming to the BIOS world using industry standards.

UEFI HIGHLIGHTS

<u>U</u>nified <u>E</u>xtensible <u>F</u>irmware <u>I</u>nterface (UEFI)

- OS-to-Firmware interface specification

- Abstracts platform from OS

- Includes modular driver model

- Compatible by design

- Modular and extensible

- Complements existing firmware & OS interfaces

OS Loader

UEFI

Platform
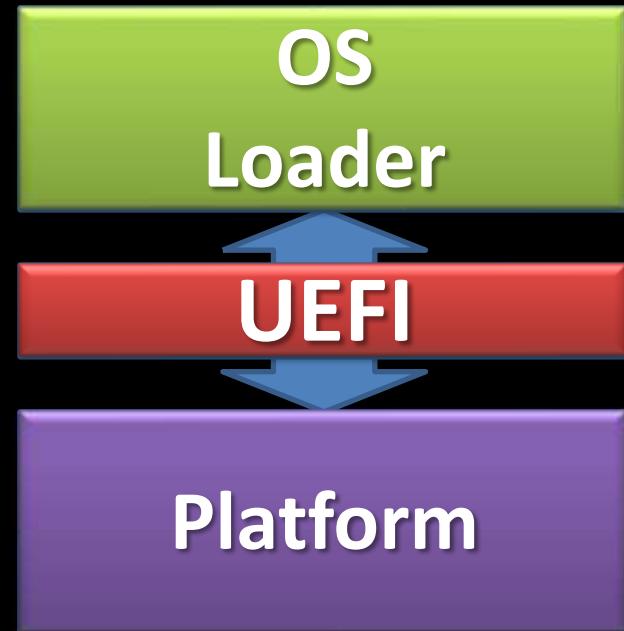
LEVERAGING UEFI ADVANTAGES

Industry Standard

Backed by over 150 member companies

C Language Development

OS & CPU independent with modern interfaces

Architecture Independent

No 16-bit … built for today's 32/64-bit systems

OVERCOMING LEGACY BIOS LIMITS
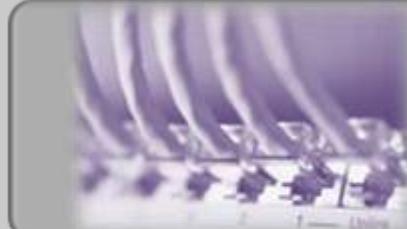
Drive Size Limitations

UEFI removes 2.2TB MBR partition limits using GPT

Networking

UEFI specification supports IPv4 and IPv6 networking ...
without the OS

Pre-Boot Applications

GUI or text tools for provisioning, recovery and diagnostics ...
without the OS

EXAMPLE: DRIVE SIZE LIMITS

- Master boot record (MBR) scheme uses 32-bit values
  - Limit is a maximum disk partition of *2.2TB*
  - It's not just a BIOS limit … OS uses the same MBR data
- New devices have massive storage needs
  - Photography, HD Video, Surveillance, Servers, …
- The UEFI solution: *GUID Partition Table (GPT)*
- GPT disks use 64-bit values to describe partitions, handling disk sizes *up to 9.4 zettabytes*
- GPT is already supported by Linux & Microsoft Windows 7

COMPATIBILITY SUPPORT MODULE

- Older OS still require "legacy BIOS" (16-bit) interfaces
- Aptio uses the *Compatibility Support Module (CSM)*
  – All 16-bit BIOS compatibility is handled by the CSM
  – The CSM is included by default in Aptio UEFI projects
- UEFI & legacy BIOS support in the same firmware … *maximum platform flexibility*
- CSM does not require changes between platforms … *easy to implement*
- CSM is modular and can be removed if it is not required … *flexible solution*

CSM AND PLATFORM CLASS

- The UEFI Forum defines four platform types ("class") based on CSM presence

- This helps identify platform compatibility with UEFI and legacy BIOS interfaces …

- Today's Aptio systems ship as *UEFI Class 2*

- Remove CSM -> UEFI Class 3

Class 0: Legacy BIOS	**Class 1: UEFI with CSM only**
Class 2: Both UEFI and CSM	**Class 3: UEFI Only (no CSM)**

AMI PRODUCTS LEVERAGING UEFI

Aptio

UEFI Solution for any x86 BIOS application

AMI Provisioning

GUI pre-boot apps, based on UEFI

AMIDiag for UEFI

Pre-boot diagnostics for test and burn-in without an OS
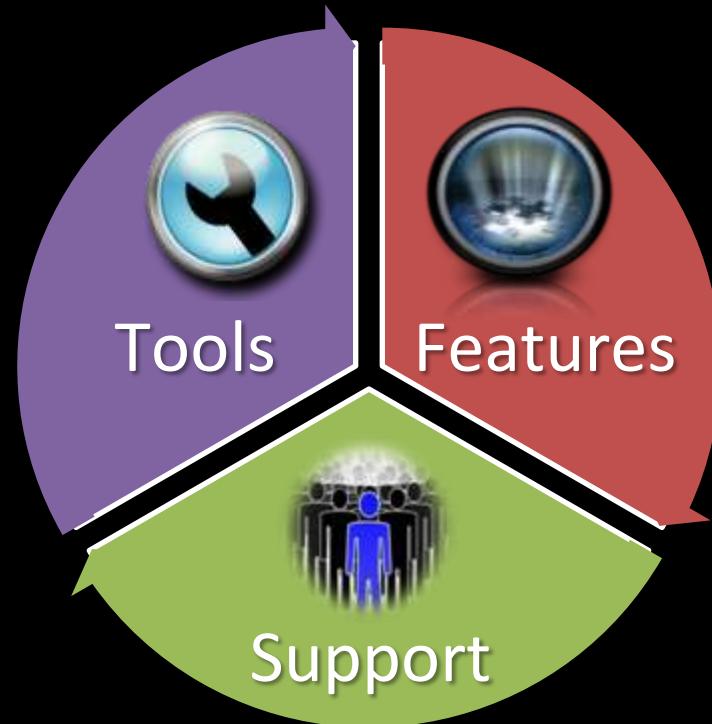
# APTIO DEVELOPMENT TOOLS

- A <u>complete</u> BIOS solution

✓ Visual eBIOS (VeB) for *rapid BIOS/UEFI porting*

✓ AMIDebug Rx enables *USB based debugging at every phase* … from development to deployment

✓ Full suite of *BIOS ROM modification tools* and *factory deployment utilities*

APTIO FEATURES VIA EMODULE

- AMI *invented the eModule* in 2001
- eModules provide *drop-in BIOS & UEFI features* at the source level
- Examples …
  - Graphical setup client for a *custom BIOS setup experience*
  - Fast Boot provides *faster boot time without any BIOS porting*
  - Aptio Secure Firmware Update (ASFU) *prevents runtime firmware attacks for additional BIOS security*
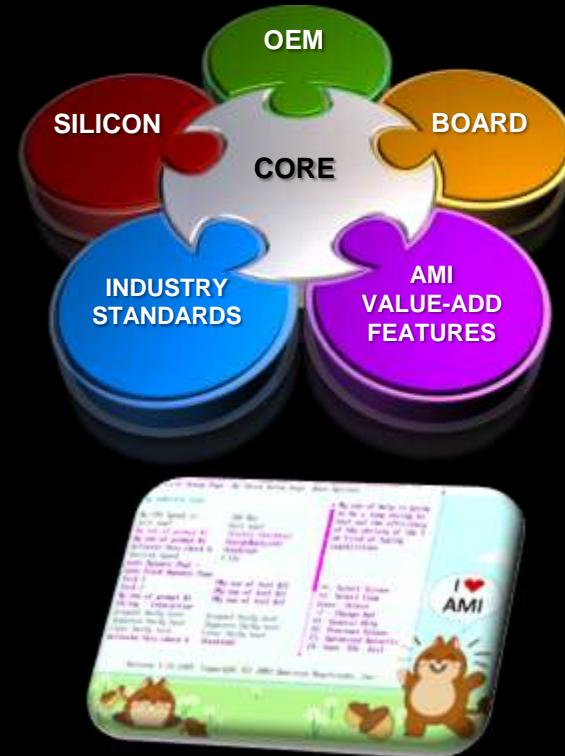
REDUCE SERVICE COSTS USING UEFI

- *AMI Provisioning*
  - Rescue, update & diagnose
  - Graphical interface in UEFI
  - Works *better than a recovery DVD*
  - Runs *even when the OS has failed*

- *AMIDiag for UEFI*
  - Platform testing *without an OS*
  - Embed diag in BIOS or run on disk

BIOS & UEFI DEVELOPMENT

- AMI helps customers manage BIOS & UEFI development by delivering a full solution
  - *Providing tools that reduce the complexity of UEFI*
  - Development Tools & Modular Source Code
  - Debugging and Diagnostic Tools
  - Utilities for BIOS ROM File Maintenance
  - Utilities for the Manufacturing Environment
- For developers working with AMI, more extensive training is offered for BIOS & UEFI

RESOURCES

- The Unified EFI Forum – www.uefi.org

- The UEFI Primer @ uefi.org

- Learning Center @ uefi.org

- Aptio information @ www.ami.com

- AMIDiag for UEFI information @ www.ami.com

- AMI Provisioning information @ www.ami.com

- "Ask a BIOS Guy" on Twitter @askabiosguy
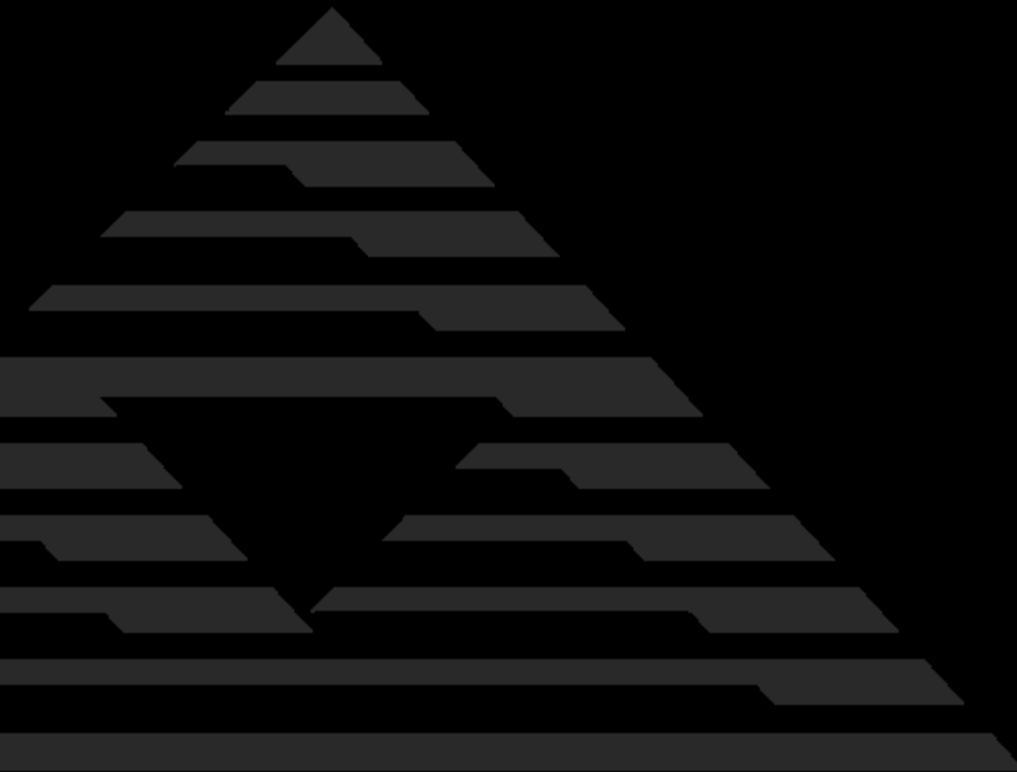
5555 Oakbrook Parkway
Suite 200
Norcross, GA 30093

www.ami.com